# Exclusive: National Guard called in to thwart cyberattack in Louisiana weeks before election

reuters.com/article/us-usa-election-cyber-louisiana-exclusiv/exclusive-national-guard-called-in-to-thwart-cyberattack-in-louisiana-weeks-before-election-idUSKBN27823F

Christopher Bing

Technology News
Updated

By Christopher Bing

6 Min Read

(Reuters) - The Louisiana National Guard was called in to stop a series of cyberattacks aimed at small government offices across the state in recent weeks, according to two people with knowledge of the events, highlighting the cyber threat facing local governments in the run up to the 2020 U.S. presidential election.

FILE PHOTO: Silhouettes of laptop users are seen next to a screen projection of binary code are seen in this picture illustration taken March 28, 2018. REUTERS/Dado Ruvic/Illustration/File Photo

The situation in Louisiana follows a similar case in Washington state, according to a cybersecurity consultant familiar with the matter, where hackers infected some government offices with a type of malware known for deploying ransomware, which locks up systems and demands payment to regain access.

Senior U.S. security officials have warned here since at least 2019 that ransomware poses a risk to the U.S. election, namely that an attack against certain state government offices around the election could disrupt systems needed to administer aspects of the vote.

It is unclear if the hackers sought to target systems tied to the election in Louisiana or were simply hoping for a payday. Yet the attacks raised alarms because of the potential harm it could have led to and due to evidence suggesting a sophisticated hacking group was involved.

Experts investigating the Louisiana incidents found a tool used by the hackers that was previously linked to a group associated with the North Korean government, according to a person familiar with the investigation.

That tool was described to Reuters as a remote access trojan, or RAT, used to infiltrate computer networks. But cybersecurity analysts who have examined this RAT - known as “KimJongRat” - say some of its code had been publicized in a computer virus repository, where hackers could copy it; making attribution to North Korea less certain.

While staff at several government offices in northern Louisiana were successfully compromised as part of the campaign, according to the two people familiar with the incident response, the cyberattack was stopped in its early stages before significant harm was done.

The Louisiana National Guard declined to comment on the incidents. A spokesman for the Louisiana State Police said they were called in to investigate the cyberattacks, but declined further comment. The Governor’s office said they could not comment on an ongoing investigation.

Tyler Brey, a spokesman for the Louisiana Secretary of State’s office, said Louisiana is a “top down state,” where election data is centrally stored at the secretary of state’s office, which can make it easier for election officials to recover from cyberattacks.

One person familiar with the events said they assessed the hacker’s objective was to infect computers with ransomware, but added that it was difficult to determine because the attack was stopped in its early phases.

If so, Louisiana wouldn’t be the first. Over the last year, several U.S. cities have been victimized by ransomware, including: incidents in Baltimore, Maryland, and Durham, North Carolina.

## THE BIG QUESTION

Jen Miller Osborn, deputy director of threat intelligence for U.S. cybersecurity company Palo Alto Networks, tracked a hacking group last year that used KimJongRat. She said it would be “atypical” for the group she’s studied to conduct a cyber operation for financial gain.

A prior cybersecurity research report in 2013 by Luxembourg firm iTrust Consulting noted that KimJongRat was written with Korean computer code which carried references to the North Korean leader’s family members.

Emotet, an increasingly common trojan often used against banks, was also deployed by the attackers and found on computers in Louisiana. When staff were hacked, their email accounts would sometimes be co-opted by the hackers to send malware to other colleagues.

On October 6, the Homeland Security Department’s cybersecurity division, known as CISA, published an alert saying Emotet was being used to target numerous local government offices across the country.

In recent cases where cybercriminals have gone after local government offices as the election approaches, like in Washington, U.S. officials along with technology companies such as Microsoft Corp are racing to better understand if the hackers share connections with foreign intelligence agencies from Russia, Iran, China and North Korea.

“It’s a very interesting question and something we are digging into and trying to find data, information, and intelligence that would help us understand that better,” Microsoft Vice President Tom Burt said in a recent interview.

“There are a small number of criminal groups who are responsible for the majority of the ransomware attacks and so understanding who they are, how they’re organized, who they work with, where they are operating from, is something we’re working on,” Burt added.

Microsoft is among a select group of cybersecurity companies helping respond to the attacks in Washington, where they’ve offered cybersecurity protection software for free to local government officials until the election, according to a person familiar with their response.

A Microsoft spokesperson declined to comment on the company’s work there.

Reporting by Christopher Bing; editing by Chris Sanders and Edward Tobin

Our Standards: The Thomson Reuters Trust Principles.

for-phone-onlyfor-tablet-portrait-upfor-tablet-landscape-upfor-desktop-upfor-wide-desktop-up