Explainer: Not all cyber threats equally worrisome

January 10 2020, by Eric Tucker

This Saturday, Oct. 7, 2017, file photo shows a polling place at Southside Elementary in Huntington, W.Va. State election officials in at least two dozen states, including West Virginia, have seen suspicious cyber activity in the first half of January 2020, although it's unclear who was behind the efforts and no major problems were reported. (Sholten Singer/The Herald-Dispatch via AP, File)

West Virginia reported unusual cyber activity targeting its election systems. The Texas governor said the state was encountering attempted "attacks" at the rate of "about 10,000 per minute" from Iran. Information technology staff in Las Vegas responded to an intrusion, though the city says no data was stolen.

All told, state election officials in at least two dozen states saw suspicious cyber activity last week, although it's unclear who was behind the efforts and no major problems were reported.

Long before a targeted U.S. strike killed a top Iranian general, there were already concerns about foreign efforts to hack American institutions and its elections. The conflict with Iran has only exacerbated those fears.

Yet as the recent spate of reports makes clear, not all suspicious cyber activities are equally troublesome, the work of a foreign government or a precursor to the type of Russian interference seen in the 2016 election on behalf of President Donald Trump.

A look at what kinds of cyber activities are worrisome—and what are not:

WHAT SORT OF ACTIVITY IS THIS?

Generally speaking, what the states are reporting are efforts to probe their networks for vulnerabilities, or weaknesses that can be exploited for potential intrusion.

"Think of it in the real world as a bank robber walking by a bank—first thing they're going to do is case the joint, and the same thing happens in the digital space," said former FBI agent Anthony Ferrante, who served as director for cyber incident response at the White House's National

Security Council.

The culprits are doing the cyber equivalent of wiggling a doorknob, said Ferrante, the global leader of the cybersecurity practice at FTI Consulting.

Scanning for network vulnerabilities is remarkably common. In fact, federal officials believe election officials in all 50 states were probably targeted during the 2016 election, though the number of known breaches—including in Illinois and a couple of counties in Florida—was significantly more modest. A Senate intelligence committee report found no evidence that votes or voting registration systems were altered.

IS THE ACTIVITY WORRISOME?

It can be, to the extent that it demonstrates that a hacker has set his sights on exploring—and possibly returning to—a particular network, and especially if a target is part of the country's critical infrastructure.

Much depends as well on the volume and frequency, since repeated, unwanted contact with a website can overwhelm an internet-connected server, effectively shutting it down in what is known as a distributed denial of service, or DDoS attack.

In general, though, when it comes to poking around a network, "I would certainly put it in a less severe category of threat activity than, say, an intrusion," said Luke McNamara, a principal analyst at FireEye, a cybersecurity firm.

It's "certainly not evidence that an intrusion has taken place or that they've been compromised," he added.

___

In this Nov. 6, 2018, file photo, people vote at a polling place in Las Vegas. State election officials in at least two dozen states, including Nevada, have seen suspicious cyber activity in the first half of January 2020, although it's unclear who was behind the efforts and no major problems were reported. (AP Photo/John Locher, File)

THE THREAT OF SPEARPHISHING

Experts say many major hacks originate not with network scans but with spearphishing emails—messages that appear legitimate but that actually launch malicious software that, once opened, can give an intruder access to the network or trick a target into unwittingly surrendering a network password.

It was a ploy used by Chinese hackers charged by the Justice Department in 2014 with hacking into the networks of major American corporations and stealing their trade secrets, and with Russian hackers who stole emails belonging to the Hillary Clinton campaign during the 2016 presidential election.

"That might be evidence of a more targeted effort. It may be that one of those is going to get through, and all you need is one," said Suzanne Spaulding, former under secretary for the National Protection and Programs Directorate at the Department of Homeland Security.

She said the first big question that organizations and governments have to confront is, "Do you have evidence that your system was breached? That's what you're really worried about."

The tactic is also significantly more subtle than pinging a network, and thus a preferred technique for sophisticated hackers loath to raise alarms.

"If your attempt is to try to compromise an organization, you probably want to be a little more surreptitious about it," McNamara said.

___

THE THREAT TO PUBLIC CONFIDENCE

Practically speaking, there's a big difference between scanning a network for vulnerabilities and actually breaking into it and extracting sensitive information.

But experts say even scans may nonetheless benefit Russia, or any other country looking to undermine faith in elections, particularly if unschooled officials sound unwarranted alarms. The American public

may not appreciate the distinction between activities that may be fairly routine and full-blown cyberattacks.

"I believe that one of Russia's objects is to undermine public confidence in the legitimacy of the outcome just as a way of weakening us," said Spaulding, now a senior adviser at the Center for Strategic and International Studies.