Cyber-attacks rising in Utah, likely due to NSA facility (Update)

February 6 2015, byBrady Mccombs

(AP)—Utah state officials have seen what they describe as a sharp uptick in attempts to hack into state computers in the last two years, and they think it related to the NSA data center south of Salt Lake City.

The increase began in early 2013 as international attention focused on the NSA's $1.7 billion warehouse to store massive amounts of information gathered secretly from phone calls and emails.

"In the cyber world, that's a big deal," Utah Public Safety Commissioner Keith Squires told a state legislative committee this week.

While most of the attempts are likely innocuous, cyber experts say it is possible low-level hackers, "hactivists" unhappy with the NSA's tactics, and some foreign criminal groups might erroneously think the state systems are linked to the NSA.

"Maybe these hackers are thinking: 'If we can attack state systems, we can get info that NSA isn't releasing," said Richard Forno, director of the University of Maryland, Baltimore County's, graduate cybersecurity program.

The state tracks the attempts with an automated system it purchased after a breach of health care information in 2012. The system detects, stops and counts the attempts to get into the computers, Squires said.

With that new equipment in place in January 2013, the state was seeing an average of 50,000 a day with spikes up to 20 million, Squires told The Associated Press. In February 2013, the number rose to an average of 75 million attacks a day, with up to 500 million on some days.

Attacks include direct attacks on websites, emails fishing for passwords, and something called "port scans," where people probe a computer looking for weak spots.

The NSA didn't immediately have any comment about the attacks.

Tim Junio, a cybersecurity researcher at Stanford University, said what officials refer to as "attacks" are likely just "noise from low-tech people rather than concerted efforts for meaningful foreign intelligence collection."

But both Forno and Junio agree the NSA data center could draw the attention of hackers who think they can target state-run utilities that power the center. Being able to disrupt an NSA operation in any way would bring international notoriety to a foreign state or criminal group, Junio said.

State officials acknowledge that part of the increase is driven by an overall rise in hacking across the country. Hackers' motivations vary, and it was impossible to determine what might be behind the activity in Utah.

Some steal personal information, like customer lists, to commit identity theft. Some take control of email servers to steal messages, send unwanted advertising or disguise the origin of their communications. Some steal corporate or government secrets from email or cloud servers, or use unlocked file servers as digital "dead drops" for their hacking tools, pirated movies, stolen files and more.

For hackers seeking notoriety, the NSA would be a prized target because it employs the world's best hackers and routinely gives advice about how to keep computers safe from online criminals.

Citation: Cyber-attacks rising in Utah, likely due to NSA facility (Update) (2015, February 6) retrieved 25 April 2024 from
https://phys.org/news/2015-02-cyber-attacks-utah-due-nsa-facility.html