PHYS.ORG

NKorea outage a case study in online uncertainties

December 24 2014, byRaphael Satter

South Korean army soldiers watch a TV news program reporting North Korean websites suffer shutdown, at the Inter-Korean Transit Office near the border village of Panmunjom in Paju, South Korea, Wednesday, Dec. 24, 2014. Key North Korean websites suffered intermittent outages Tuesday after a nearly 10-hour shutdown that followed a U.S. vow to respond to a crippling cyberattack on Sony Pictures that Washington blames on Pyongyang. The letters read " North Korean internet suffers shutdown." (AP Photo/Ahn Young-joon)

North Korea's microscopic corner of the Internet has had a rough couple of days, suffering seven outages in the last 48 hours, according to one Web traffic monitor.

The mysterious problems have some talking of a retaliatory cyberattack by the United States, which holds Pyongyang responsible for last month's spectacular hack of Sony Pictures. American officials have fueled speculation with vague denials, but security experts say North Korea's Internet infrastructure is so skeletal that even amateurs—or a simple glitch—could have brought it clattering down.

"A large city block in London or New York would have more IP (Internet Protocol) addresses than North Korea," said Ofer Gayer, a security researcher at Redwood Shores, California-based Incapsula Inc. He said that if the network was targeted by a kind of distributed denial-of-service—or DDoS—attack, the list of suspects is endless.

"Any kid that knows how to run a small-sized DDoS amplification attack can do it from his home."

For many, the uncertainty over the outage—and lingering doubts over who hacked Sony—illustrates how little we can really know about attacks in the Information Age.

"This whole incident is a perfect illustration of how technology is equalizing capability," Bruce Schneier, a respected security expert, said in a blog post. "In both the original attack against Sony, and this attack against North Korea, we can't tell the difference between a couple of hackers and a government."

Here's what is known:

FOR TWO DAYS, NORTH KOREA STRUGGLED TO STAY ONLINE

After spending a significant chunk of Monday offline, North Korea's Internet had two short outages Tuesday morning, according to Jim Cowie, the chief scientist at Dyn Research, an Internet performance company.

Cowie characterized the outages as a "return to instability," and said they were the same type of outages that caused the original disruption.

Hiccups continued until Wednesday. Internet monitor BGPmon says it has detected a total of seven interruptions, with the last hour-long outage reported between 6:30 and 7:45 GMT.

IT DOESN'T TAKE MUCH TO KNOCK NORTH KOREA OFF THE WEB

North Korea has a tiny online footprint, thousands of millions of times smaller than that of the United States or even archrival South Korea. Gayer, the Incapsula researcher, pegged the country's total bandwidth at 2.5 gigabits per second, a minuscule amount of traffic which could easily be overwhelmed by a denial-of-service attack. Only last week, a London teenager pleaded guilty to a cyberattack against an anti-spam group which clocked in at 300 gigabits per second.

SPECULATION IS RAMPANT

U.S. officials have refused to be drawn over the online mischief, feeding speculation that American retribution may be to blame for North Korea's Internet problems.

"Ask the North Koreans if their Internet wasn't working," said U.S. State Department representative Marie Harf in response to questions about the outages on Tuesday. "I would check with them."

The attack doesn't fit the pattern of an American cyber-strike, said Dan Holden of Arbor Networks, which works to block denial-of-service attacks. He said online activists may be to blame, and social media chatter provides some support for the claim.

One prominent account linked to Anonymous, the amorphous collective of self-appointed cyber-vigilantes, briefly claimed credit for knocking North Korea offline before it was itself was yanked from the Internet by Twitter. Rival claims—from obscure groups carrying names like "Lizard Squad" or "Gator League"—were even harder to assess.

THIS HAS HAPPENED BEFORE

North Korea's Internet has gone dark before. In March 2013 the nation experienced connectivity problems for the better part of a day and a half.

The North Korean government blamed the United States for the problems, but their cause has never been publicly confirmed.

Citation: NKorea outage a case study in online uncertainties (2014, December 24) retrieved 3 September 2024 from
https://phys.org/news/2014-12-nkorea-outage-case-online-uncertainties.html