IF A CLOSE US ALLY BACKDOORED JUNIPER, WOULD NSA TELL CONGRESS?

You may have heard that Juniper Networks announced what amounts to a backdoor in its virtual private networks products. Here's Kim Zetter's accessible intro of what security researchers have learned so far. And here's some technical background from Matthew Green.

As Zetter summarizes, the short story is that some used weaknesses encouraged by NSA to backdoor the security product protecting a lot of American businesses.

> They did this by exploiting weaknesses the NSA allegedly placed in a government-approved encryption algorithm known as Dual_EC, a pseudo-random number generator that Juniper uses to encrypt traffic passing through the VPN in its NetScreen firewalls. But in addition to these inherent weaknesses, the attackers also relied on a mistake Juniper apparently made in configuring the VPN encryption scheme in its NetScreen devices, according to Weinmann and other cryptographers who examined the issue. This made it possible for the culprits to pull off their attack.

As Green describes, the key events probably happened at least as early as 2007 and 2012 (contrary to the presumption of surveillance hawk Stewart Baker looking to scapegoat those calling for more security). Which means this can't be a response to the Snowden document strongly suggesting the NSA had pushed those weaknesses in Dual_EC.

I find that particularly interesting, because it suggests whoever did this either used public

discussions about the weakness of Dual_EC, dating to 2007, to identify and exploit this weakness, or figured out what (it is presumed) the NSA was up to. That suggests two likely culprits for what has been assumed to be a state actor behind this: Israel (because it knows so much about NSA from having partnered on things like StuxNet) or Russia (which was getting records on the FiveEyes' SIGINT activities from its Canadian spy, Jeffrey Delisle). The UK would be another obvious guess, except an Intercept article describing how NSA helped UK backdoor Juniper suggests they used another method.

Which leads me back to an interesting change I noted between CISA — the bill passed by the Senate back in October — and OmniCISA — the version passed last week as part of the omnibus funding bill. OmniCISA still required the Intelligence Community to provide a report on the most dangerous hacking threats, especially state actors, to the Intelligence Committees. But it eliminated a report for the Foreign Relations Committees on the same topic. I joked at the time that that was probably to protect Israel, because no one wants to admit that Israel spies and has greater ability to do so by hacking than other nation-states, especially because it surely learns our methods by partnering with us to hack Iran.

Whoever hacked Juniper, the whole incident offers a remarkable lesson in the dangers of backdoors. Even as FBI demands a backdoor into Apple's products, it is investigating who used a prior US-sponsored backdoor to do their own spying.