Twitter Thread by Matthew Green



Matthew Green
@matthew_d_green

I couldn't tweet a better description than the headline for this piece: After SolarWinds breach, lawmakers ask NSA for help in cracking Juniper cold case.

For those who haven't heard this story, the context here is back in 2015 hackers broke into the source code repository of Juniper's NetScreen firewalls and introduced serious vulnerabilities. 1/

Everyone has heard of the SolarWinds supply chain attack, but almost nobody outside our little community remembers Juniper. We don't even know who the ultimate victim was. And there's a reason for that. 2/

The reason is simple: following the Juniper hack, the FBI and Juniper put a tight lid on everything. Nobody, including members of Congress, were able to get straight answers about who did it or what the target was. So it vanished from our collective memory. 3/

This has real consequences. To some extent our lack of preparedness for SolarWinds is a direct result of our government's decision to pretend that the previous major supply-chain attacks didn't happen. 4/

Why has the Juniper attack been buried by secrecy? There are two possible answers. One has to do with the nature of the hack, which very likely repurposed an existing backdoor in NetScreen firewalls. The other has to do with the ultimate target. 5/

Regarding the first, we know that Juniper included a *likely* crypto backdoor based on an NSA algorithm called Dual_EC_DRBG even before the hack. We also know that the attackers repurposed that code to use new public keys of their choosing. This is very embarrassing. 6/

(We know this because people on Twitter and co-authors of mine were able to reverse engineer the details from the published firmware images. See here for a nice explanation. https://t.co/CPHw8oA6zA)

The second answer to "why was this buried" is much more speculative. It has to do with the identity of the actual target(s) that were attacked using the NetScreen vulnerabilities. We don't know who they are, and they might be important. 8/

I continue to harbor the conspiracy theory that the Office of Personnel Management hack was in some way related to Juniper, based solely on the timing and some equipment manifests from that agency. I'm probably wrong, but that would be a hell of a reason to cover things up. 9/

The point here is that with attacks like this and a secrecy response, we're screwed. Until we know what happened in these cases, we can't learn from it. This makes us defenseless, and you can bet our adversaries prefer it that way. 10/

It's as though the US government decided to react to Pearl Harbor by covering things up. You have to imagine that history would look a lot different. Hopefully we'll stop making this mistake. //fin