Twitter Thread by Lulu Friesdat

Lulu Friesdat
@LuluFriesdat

#SolarWinds hack. Thread.

1. Dominion Voting Systems, a voting machine vendor used in #Election2020, is a Solar Winds client. It does not use Orion, the product at the center of the hack. via attorney Paul Lehto

Solar Winds list of clients is now hidden

2. Unknown if #hacking investigation is expanding to all #SolarWinds clients, like Dominion Voting Systems. #ElectionSecurity #ElectionProtection #Election2020results

3. "early signs indicate the reach of the stealthy supplychain attack will have substantial aftershocks; #SolarWinds claims to have 300,000 customers, inc. /National Security Agency all 5 branches of the U.S. military & entities in /health tech telecommunications media & finance"

4. We discuss the #SolarWinds breach in our #ElectionProtection forum on Tuesday with Election & Cyber expert @rad_atl

https://t.co/jj0zK2i2gJ (46 mins in)

5. Department of Homeland Security is one of the hacked agencies. CISA (a DHS sub-agency) assured the public that “The November 3rd election was the most secure in American history." Meanwhile DHS may have been compromised itself for as much as 9 months. https://t.co/dU6ViAI4h1

6. "hackers responsible for the infiltration of SolarWinds are some of the most capable hackers FireEye says it has ever observed/but it’s alarming that the U.S. government’s / intel & natl security apparatus was not alert to the espionage operation" https://t.co/R3Z1U5zwaW

7. The hack was not 1st reported by US intel, but by a private company FireEye, a private security firm that found it had been hacked itself. https://t.co/PaZ0r5tT4K

#ElectionSecurity #ElectionProtection #Election2020results #SMARTelections

8. "hackers, had penetrated FireEye's servers and made off with its crown jewels: the tools it uses to test other companies' defenses. Armed with those penetration tools, hackers could potentially identify which of their methods will pass FireEye's gaze undetected." #Election2020

9. Much of the penetration was done by compromising official software downloads "US government networks were compromised: by installing tainted downloads – " This can also be done with voting machines as well - because they have to be updated for each election. #ElectionIntegrity

10. So the argument that is commonly used that voting machines are secure because they are not connected to the internet is false. It's good to keep voting systems offline - but election best practices must take into account that almost any system can eventually be hacked.

11. That is why meticulous, thorough post-election auditing of ballots that are hand-marked by voters whenever possible is so important - because that is how security experts recommend a system can be checked for accuracy to verify no hacking or mistakes have occurred. #Elections

12. Touchscreen ballot-marking devices like Dominion ICX (Georgia) and ExpressVote XL (Philly & NY - pending cert) are NOT good to use as a primary voting system. Because the computer creates the ballot, there's no way to use an audit of ballots to check for #hacking & errors.