Twitter Thread by SwiftOnSecurity



SwiftOnSecurity
@SwiftOnSecurity

The SolarWinds hack is a fundamental challenge, but I went into work yesterday focused on the same basics.

This may be a game-changer for policy and industry, but the essentials are what make the difference here. It revalidates basic visibility and monitoring. Same as before.

I do not see complex networks as they exist today as bastions where you can close your eyes anywhere assuming you're fine.

What if an attacker just compromised Orion with an exploit like a normal attacker? Or pivoted into its memory space from elsewhere?

What's the difference?

You've got to have pretty incredible network segmentation and administrative tiering and insider threat program before this kind of attack is the biggest risk to worry about.

That doesn't mean it's not incredibly serious. But we're failing way worse than this every single day.

This is a hard dichotomy to talk about without sounding dismissive, but I think it's worth bringing up. Be ever more mindful, but keep our foot on the gas on our fundamentals without letting up.

I'm putting some thoughts together, but I can't get over the fact _they didn't even try to infect your network if it looked like you were watching the machine_.

Like, we should be screaming about this. They know this shit works against them.

Note: This is not saying FireEye and other networks did not have monitoring in place, but it may not have been with tools in their list of "nope I'm not even trying" list.

The fact they hit FireEye seems like a massive mistake since they have internal custom tooling.

Everyone is doom and gloom while I'm like Neil Patrick Harris in Starship Troopers where he puts his hand on the bug and says "they feel fear" and everybody cheers.

It's worth saying, cyber hygiene may be in refutation of buzzwords, but it's not the end-all-be-all of IT protection.
You do need top-flight systems and people at the edges looking for the exceptional vectors.
But I want to keep harping on these fundamentals for everybody else.