Twitter Thread by Dannielle (Dossy) Blumenthal PhD

Dannielle (Dossy) Blumenthal PhD
@DrDannielle

If it's "Russia" why are they investigating if the execs were in on it?

"HAGENS BERMAN, NATIONAL TRIAL ATTORNEYS, Investigating SolarWinds (SWI) $285 Million Insider Stock Sales, Knowledge of Hack in Orion Products, Encourages SWI Investors with Losses to Contact Firm Now"
https://t.co/n7AHw51r4m

SolarWinds report (Feb 2020): "2020 Key Findings
For the fifth year in a row, careless and untrained insiders are the leading source of security threats for public sector organizations"

https://t.co/TjgcuaBzUb

"'Security is everyone's job, but holding the team accountable is lacking. Until there are real individual accountability regimens in place, the network will remain at risk.'
- Division Chief, Federal Civilian"

Again insiders are the top threat, why ignoring in public rhetoric?

https://t.co/603WejHoYG

It doesn't add up https://t.co/1MNMdHqyH6

> Check insider threat!
> 1. 8/19: SolarWinds\u2019 Orion acquired DOD
> 2. Late 2019: SW warned solarwinds123= pwd
> 3. Spring 2020: Spy hack
> 4. Hackers snoop
> 5. 12/7 Top investor SilverLake dumps $158M stock
> 6. 12/13 FireEye Security details hack in blog
> 7. 12/14 Gov pulls plug SW Orion
>
> — Dannielle (Dossy) Blumenthal PhD (@DrDannielle) December 16, 2020

Why would SolarWinds ignore this warning?

https://t.co/VVQ7TqlUzW

Important article

“The SolarWinds Perfect Storm: Default Password, Access Sales and More” https://t.co/a1xHU46nON via @threatpost

“Orion is a product with such market dominance that company CEO Kevin Thompson bragged on an October earnings call that “.....We manage everyone’s network gear.”

“In addition to its overall footprint, perhaps what made SolarWinds the most attractive vector for the attackers however is its sheer reach into customer networks.”

“access to the full network....Compromising SolarWinds makes sure an attacker does not have to worry about firewalls and other preventative security solutions.... It knows EVERYTHING on your network.”

- Marcus Hartwig, manager of security analytics, Vectra

“users of SolarWinds are IT/network admins with privileged access accounts”

“cybercriminals were spotted hawking access to SolarWinds’ infrastructure in underground forums, as far back as 2017”

“One of the access-dealers, they said, was the notorious Kazakh native known as ‘fxmsp’”

“German newspaper flagged the fact that SolarWinds has a support page advising users to disable antivirus scanning” (!) in Orion folders

“authorities have identified fxmsp as a 37-year-old Kazakhstan citizen named Andrey Turchin” https://t.co/TH0AnXfREl

“established backdoors to corporate networks and then sold them in cybercrime forums for thousands to hundreds of thousands of dollars”

“Think of almost any kind of company and there’s a good chance a prolific, financially-motivated hacker known as Fxmsp has broken into it, or attempted to” https://t.co/WpOWvufeHF

“starts by scanning for open Remote Desktop Protocol ports and then brute-forcing their way into networks. They then steal administrative credentials and modify antivirus software settings to make sure their malware remains undetected.” https://t.co/TH0AnXfREl

“sold backdoor access to hundreds of corporate networks in 44 countries via Russian-language underground forums” https://t.co/pRU52RSMy1

https://t.co/6Ex9IpsZPu

Remember the Equifax hack

https://t.co/m7yWUOxHFH

“On March 7, 2017, the Apache Software Foundation announced that some versions of its Apache Struts software had a vulnerability that could allow attackers to remotely execute code on a targeted web application.”