FALLOUT FROM THE SOLARWINDS SUPPLY CHAIN COMPROMISE

It's an ill wind that blows no good, and profits nobody. That old nautical phrase popped into my head when I heard about the SolarWinds Orion supply chain compromise. Yet this may be one case where something good results from something very bad.

I read recently that the hackers likely gained access using compromised credentials and/or a third party application that took advantage of a zero-day vulnerability. The SolarWinds' CEO later confirmed that "suspicious activity" in his Office 365 email account allowed the bad actors to access and exploit the Orion software development environment. It's believed the hackers first tested their ability to insert malicious code into Orion network management software as early as October 2019. The hackers apparently had access to the company's emails for NINE months.

"So what?" you might say. Why does it matter for the rest of us, and the mainframe world in particular?

The hack was clearly very bad news for the eight US federal agencies affected, which included the FBI and the Pentagon, along with up to 18,000 other SolarWinds customers attacked with malware. Systems were monitored, data and IP harvested.

In fact, it's been reported since that around one-third of the private sector and government victims of this "colossal hacking campaign" had no direct connection to SolarWinds at all. There was probably a realization by many senior IT and security people that they had escaped by the skin of their teeth. This could have happened to anyone; you didn't even need to be an Orion software

customer. That is a “near-hit” in my mind rather than a “near-miss”.

Is there a bright side to all this? Perhaps. The compromise may have some positive outcomes by shining an even harsher light on the complacency that still exists when it comes to security, and especially the different security standards that are applied to development/supplier systems (“not really important or at risk, so why bother?”) compared to in-house production systems (“we must protect our crown jewels”).

Such attitudes continue to hamper ‘Zero Trust’ approaches, and at a time when an increasingly connected world means rising threat levels through supply chain attacks. The bad actors don’t need to get to your production systems at all, which may be tightly protected. Instead, they can look to what may be a softer target: the poorly-protected dev systems of a supplier or anyone else in your supply chain. And you won’t even know it’s happened until it’s too late.

James Stanger of the Computing Technology Industry Association (CompTIA) hit the nail on the head when he described the problem thus: “Most organizations continue to pursue traditional measures based on a firewall-first, signature-based, trusted-partner mindset.” He describes this old-school BAU approach as ‘Cowboy IT’, which he defines as “underutilization of modern tools, over-reliance on old ones and a lack of proper monitoring.” Does that sound familiar?

Securing the supply chain has become a hot topic, and we can do better. We need to lift our gazes from the threats that are closest to us - once they have been mitigated, of course – to scan the horizon, imagine what else could happen in our extended environment, and ask searching questions of partners and suppliers. All systems have to be treated as production systems, with better monitoring, more threat intelligence, and making Zero Trust the order of the day – via access rights and applying the principle of least privilege (PoLP), through more rigorous password policies, using Extended Detection and Response (XDR) capabilities, and more.

SolarWinds seems to have got the memo. In moves to lock the stable door long after the horse has bolted, the company is planning to better secure itself. This includes upgrading to “stronger and deeper endpoint protection”, expanding its Security Operations Center, strictly enforcing multi-factor authentication (MFA), expanding the use of a privilege access manager for admin accounts, and increasing pre-procurement security reviews of all vendors. It’s a start.