SolarWinds Hack Is A Seminal Event Of The Digital Age

Dec 23rd 2020

SolarWinds, of Austin, Texas, provides network-monitoring and other technical services to hundreds of thousands of organizations around the world, including most Fortune 500 companies and government agencies in North America, Europe, Asia and the Middle East. Hundreds of thousands of organisations around the world rely on a piece of the company's software called Orion to manage their IT networks. The software is described as a "single pane of glass" that can monitor everything in a system. Orion accounts for nearly half of SolarWinds' $750m annual revenue.

As early as March 2020, hackers gained entry into networks by getting more than 18,000 private and government users to download a tainted software update to Orion. SolarWinds said it sent an advisory to about 33,000 of its Orion customers who might have been affected, though it estimated a smaller number of customers – fewer than 18,000 – had actually installed the compromised product update. The infiltration tactic involved, known as the "supply-chain" method, recalled the technique Russian military hackers used in 2016 to infect companies that do business in Ukraine with the hard-drive-wiping NotPetya virus – the most damaging cyber-attack to date. The malware can transfer files, reboot computers and disable system services. It appears so far to have been used for espionage, albeit on a grand scale.

SolarWinds granted intruders broad access to the entire network of every system it was installed on, and persuaded many of its customers that its Orion products needed to be exempt from existing antivirus and security restrictions on their computers because otherwise it might look like a threat or be unable to function properly. This is actually an old problem—security products identifying other security products as malware. The attackers apparently made use of their initial access to targeted organizations, such as FireEye and Microsoft, to steal tools and code that would then enable them to compromise even more targets. After Microsoft realized it was breached via the SolarWinds compromise, it then discovered its own products were then used "to further the attacks on others," according to Reuters.

One of the key questions, according to western security officials, is how the hackers managed to penetrate SolarWinds. Doing so may not have been difficult - Vinoth Kumar, a security researcher, told Reuters that, last year, he alerted the company that anyone could access SolarWinds' update server by using the password "solarwinds123". Possibilities also include an insider at the company who helped the hackers gain access to its clients, or weaknesses in cyber security which meant its systems could be targeted remotely.

The breach was not discovered until December 12th when the prominent cybersecurity company FireEye, which itself also uses SolarWinds, determined it had experienced a breach by way of the software. FireEye described the malware's dizzying capabilities – from initially lying dormant up to two weeks to hiding in plain sight by masquerading its reconnaissance forays as Orion activity.

SolarWinds said it was advised that an "outside nation-state" had infiltrated its systems with malware. Officials suggested the attack has all the hallmarks of an espionage operation, designed to target central government, defence, military and intelligence institutions. It is one of the largest and most brazen hacks in American history — and it may just be the beginning of a much larger global espionage effort. Some experts believe it may take years before the hackers are completely out of the US government's networks and the full extent of their spying efforts are understood.

Sources : The Guardian, Slate, Vox, FT - Dec 15th 2020, FT - Dec 16th 2020