21 Dec, 2020

Utilities vulnerable to cyberattack even if they did not use SolarWinds software

Author **Zack Hale, Molly Christian**

U.S. electric utility companies may be vulnerable to a Russian-orchestrated cyberattack even if they were not direct clients of the firm whose tainted software was used to breach thousands of networks, according to cybersecurity experts.

Private-sector utilities are generally well-invested in so-called "front door" cyber defenses designed to safeguard the nation's critical infrastructure facilities against frontal assaults, said Stuart Madnick, founding director of the Massachusetts Institute of Technology's cybersecurity program. However, utilities can still face "side door" attacks via third-party vendors that used the SolarWinds Corp.'s Orion software at issue, Madnick said.

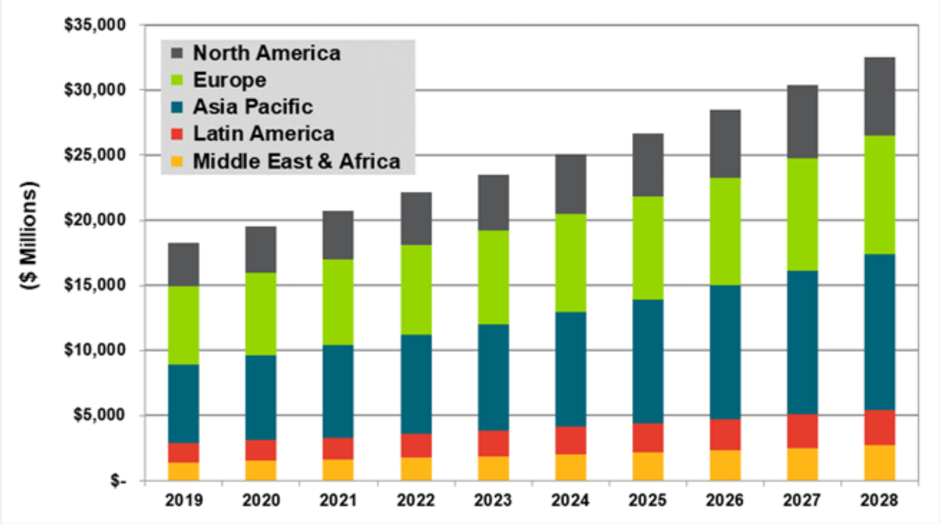
"It's not the front door attack," Madnick said in an interview shortly before the U.S. publicly named Russia as the likely perpetrator of a massive cyberattack that compromised systems used by the U.S. Department of Energy and Federal Energy Regulatory Commission, among others. "The side door says service vehicles enter here, or suppliers enter here, so they could come in through that door into the system, bypassing all the security at the front gate," Madnick said.

While the U.S. utility industry has been guarded in public statements immediately after the attack, experts say the breach is much worse than initially feared.

After FireEye Inc., a leading U.S. cybersecurity firm, on Dec. 8 first reported evidence of intruders in its system, the Electricity Subsector Coordinating Council on Dec. 14 issued a statement saying that it is "highly engaged" and has already conducted a situational awareness call on the threat. The ESCC, which is responsible for coordinating cyberattack responses between the federal government and U.S. power industry, has yet to issue any further statements.

Cybersecurity experts are warning that the full scale of the attack will likely never be known, but they are also characterizing it as one that will require huge investments in time and money to clean up.

Energy, IT, analytics, cybersecurity revenue by region, world markets (2019-2028)



As of Feb. 11, 2020.
Source: Navigant Research

"This one's worse than people realize," said Robert Lee, CEO of Dragos Inc., a leading industrial cybersecurity company. "The gravity of this is high, because it's a supply chain compromise."

Supply chain compromises can occur when companies download software updates containing malicious code, as was the case with a months-in-the-making attack orchestrated through SolarWind, a provider of networking software with numerous high-level U.S. government contracts.

One of the main logistical hurdles affected companies will need to clear is determining whether to replace SolarWinds' software with another networking solution, explained Madnick.

"They can either operate without any of the safeguards SolarWind was providing them, which means they're now more vulnerable, or they have to switch to some other system that does comparable things," Madnick said. "In either case, it's a fairly major change in your infrastructure, either to defer running SolarWind or replacing it with something else. All of these things, once again, mean time and energy."

Lee said his firm is already responding to calls from companies that do not directly use SolarWinds' software but discovered some of their vendors do. While most federal cybersecurity mandates are aimed at prevention, guidelines could be improved with an increased focus on monitoring and detection, Lee said.

News that DOE and FERC networks were breached broke as the commission proposed a new rule that would offer additional financial incentives to utilities that make cybersecurity investments going "above and beyond" what is currently required.

Last year, Navigant Research released a report projecting that the market for energy-related cybersecurity investments will grow at a compound annual growth rate of 6.6% through 2028 to more than $32 billion.